REMARKS

The arguments and amendments presented herein include the arguments and amendments Applicants discussed with the Examiner during phone interview dated February 19, 2009. The Examiner requested Applicants to submit the discussed arguments and amendments for reconsideration, which Applicants present herein. Applicants submit that the arguments and amendments presented herein make the substance of the phone interview of record to comply with 37 CFR 1.133. If the Examiner believes that further information on the interview needs to be made of record to comply with the requirements, Applicants request the Examiner to identify such further information.

1. Amended Claims Comply with 35 U.S.C. §101

The Examiner rejected claims 1-17, and 44 as directed to non-statutory subject matter (35 U.S.C. §101 on the grounds they were not tied to a statutory class or transform subject matter. (OFFICE ACTION, pgs. 2-3)

Amended claim 1 concerns operations of an interface device to use a coding key to decode and code data with respect to a target storage cartridge. During the phone interview, Applicants explained that these claimed operations concerning the operations of an interface device with respect to decoding and coding data for storage cartridges are a statutory class. Further, amended claim 1 involves the transformation of subject matter, by decrypting a coding key to use to decode and code data to read and write with respect to a target storage cartridge. In this case, the coding key is transformed from an encrypted to decrypted state and the data being written and read with respect to the target storage involves a transformation.

During the phone interview, the Examiner said that the arguments Applicants presented appear to overcome the Section 101 rejection and requested that Applicants submit for consideration, which Applicants present above.

Accordingly, Applicants request the Examiner to withdraw the Section 101 rejection.

2. Claims 1, 3-5, 7, 8, 10-16, and 44 are Patentable Over the Cited Art

The Examiner rejected claims 1, 3-5, 7, 8, 10-16, and 44 as obvious (35 U.S.C. §103(a)) over Shear (U.S. Patent Pub. 2001/0042043) and Smythe (U.S. Patent No. 5,325,430). Applicants traverse with respect to the amended claims. .

Amended claim 1 recites a method for accessing data in a read/write storage medium within one of a plurality of storage cartridges mounted into a plurality of interface devices, comprising: providing an association of at least one coding key to the plurality of storage cartridges, wherein the coding key associated with the storage cartridge is used to decode and code data in the storage cartridge; encrypting the coding keys and storing the encrypted coding keys in the storage cartridges; receiving, by a receiving interface device comprising one of the interface devices, an Input/Output (I/O) request to a target storage cartridge comprising one of the storage cartridges; mounting, by the receiving interface device, the target storage cartridge in response to the I/O request; reading, by the receiving interface device, the encrypted coding key from the mounted target storage cartridge; transmitting, by the receiving interface device, the read encrypted coding key to a host device; receiving, by the receiving interface device, the coding key encrypted by the host; decrypting, by the receiving interface device, the coding key encrypted by the host to use for the I/O request; using, by the receiving interface device, the decrypted coding key to decode data to read in the target storage cartridge including the encrypted coding key in response to the I/O request comprising a read request; and using, by the receiving interface device, the decrypted coding key to code data to write to the target storage cartridge including the encrypted coding key in response to the I/O request comprising a write request.

Applicants added the requirements of encrypting the coding keys and storing the encrypted coding keys in the storage cartridges; receiving, by a receiving interface device comprising one of the interface devices, an Input/Output (I/O) request to a target storage cartridge comprising one of the storage cartridges; mounting, by the receiving interface device, the target storage cartridge in response to the I/O request; reading, by the receiving interface device, the encrypted coding key from the mounted target storage cartridge; transmitting, by the receiving interface device, the read encrypted coding key to a host device; receiving, by the receiving interface device, the coding key encrypted by the host.

The amendments and added limitations to claim 1 are disclosed in at least paras. 50-51 and FIGs. 11 and 13 of the Specification.

Applicants submit that these amendments to claim 1 include requirements discussed with the Examiner that the Examiner indicated could distinguish the claims from the cited art and advance prosecution.

The Examiner recognized the deficiencies of Shear and cited col. 3, lines 40-62, col. 5, line 50 to col. 6, line 3 and col. 6, lines 50-63 of Smythe to overcome these deficiencies. (OFFICE ACTION, pg. 4) Applicants traverse with respect to the amended claims.

The cited col. 3 discusses a microprocessor connected via an encrypted address and data bus to a local RAM. The microprocessor includes security circuits, including an address encryptor, data encryptor, and an encryption key word. The data encryptor encrypts and decrypts data for the microprocessor.

The cited cols. 5-6 mentions an on-chip software security module as an IC card coupler interface for the computer to prevent unauthorized individuals from reading and assembling programs. The coupler software is loaded and executed by the microprocessor in encrypted form. The encryption algorithm uses a key word which is entirely stored and protected by the microprocessor. The key is unique for each initialization routine. The microprocessor reads an encrypted encryption key from an IC card and transfers the key to a key register of the DES hardware. The cited col. 6 further mentions that the device driver intercepts requests to the BIOS. When the driver intercepts an Interrupt, the device driver determines if the interrupt is associated with a file in its list, a system request or a file not listed, and places the result of the determination in a reserved memory.

Although the cited Smythe discusses how a microprocessor access a key from an IC card and transfers to a register, and encrypts and decrypts data, the cited Smythe nowhere teaches or suggests the specific claimed requirements of how an interface device manages the encryption key by transmitting the encrypted coding key to a host, receiving the encrypted coding key encrypted by the host, decrypting the coding key encrypted by the use to use to decode data to read and code data to write. Nowhere does the cited Smythe teach or suggest that the cited microprocessor accesses the encrypted coding key, then transmits to a host so that the host encrypts and returns the coding key, that the interface device then decrypts to use. Instead, the cited Smythe discusses how a microprocessor uses a key and intercepts interrupts to determine a state of the interrupt.

The Examiner found that the claimed operation of using the decrypted coding key to decrypt data to read and to code data to write comprises non-functional descriptive information. (OFFICE ACTION, pg. 5) Applicants submit that the claimed operation of the interface device using the decrypted coding key to read and write is a functional limitation describing a functional computer operation, and not non-functional descriptive material.

Applicants further submit that the cited Smythe is deficient for the reasons discussed with respect to Shear in that both discuss techniques to use to decrypt data. Nowhere do these references alone or in combination teach or suggest the claim requirements of how an interface device reads the encrypted coding key, transmits to a host, received the coding key encrypted by the host, then decrypts the coding key form the host to use to read and write data.

Accordingly, for the above reasons, Applicants submit that the independent claim 1 is patentable over the cited art because the cited Shear and Smyth does not disclose all the claim requirements.

Claims 3-5, 7, 8, 10-16, and 44 are patentable over the cited art because they depend from claim 1, which is patentable over the cited art for the reasons discussed above. Moreover, the below discussed independent claims provide additional grounds of patentability over the cited art.

Claim 3 depends from claim 1 and further requires that the association of the at least one coding key to the plurality of storage cartridges associates one key with the plurality of storage cartridges, wherein the one key encodes data written to the storage mediums and decode data read from the storage mediums of the plurality of storage cartridges.

The Examiner cited FIGs. 1A, 1B, 1C and paras. 0078-0081, 0127-0138, 0183, 0193-0199, and 0216-0220 of Shear as disclosing the requirements of the pre-amended claims. (Office Action, pg. 6) Applicants traverse.

The cited para. 0078 discusses rights management to exchange movies and games. Content is encrypted with decryption keys required to decrypt the content. The decryption keys may themselves be encrypted in an encrypted key block. The cited para. 0079 mentions that content may be secured as it is recording, such as in a camera. Reading the content for use in the rights management environment might occur at many steps along a conventional production and distribution process. Para. 0080 mentions that the storage medium carries the decryption key in a hidden portion that is used by a drive to decrypt the encrypted key block. The cited para. 0081 mentions that the video disk drive may store keys to decrypt an encrypted key block or the may be stored in a drive key store and be updateable.

The cited paras. 0127-0138 mention that different information on the medium may be encrypted using different keys and that encrypted keys may be stored on the medium to be used to decrypt the protected properties and metadata. Multiple sets of encrypted keys may be stored

on the medium to have different keys associated with different regions. A decryption key for the encrypted keys may be hidden on the medium.

The cited para. 0183 mentions that a disk may store properties or other content in protected or unprotected form, where a property is protected if it is at least in part encrypted. The disk could store both a movie as protected property and an unprotected interview, and store any number of protected or unprotected properties.

The cited paras. 0193-0199 discuss local secure execution of a control process and the use of optical media. Special hardware can be used to provide a secure execution environment to ensure safe digital commerce activities. A metering and control system, at least partially encrypted, is delivered to a user on optical media. A bill may be generated in response to transmitting information. Some or all of the content may be encrypted on the media.

The cited paras. 0216-0220 further discusses that the disk may store an encrypted key block used to decrypt properties and metadata on the disk, where different keys may be used for different data on the disk. The cited para. [0217] mentions that the cryptographic key block, which is the key used to decrypt the data, may be encrypted with one or more additional keys, and that these one or more keys need to be used to decrypt the key block to obtain the key to decrypt the data. The cited paras. [0218-0220] mentions that the keys to decrypt the encrypted key block may come from different sources. The disk may store hidden keys or the keys may be provided by the disk drive. The disk drive may have an integrated circuit decryption engine including a small secure internal key store memory having keys to use to decrypt the encrypted key block, which is then used to decrypt the content. The keys to decrypt the protected content may also be within a secure container.

The above cited Sheer discusses that a drive may access an encrypted key from disk and use the key do decrypt data from the disk. The cited para. [0081] further mentions that the disk drive may store and maintain keys used to decrypt an encrypted key block, and that a drive key store may be updateable using a communication path. The cited para. [0217] mentions that the key block having the key to decrypt the data may be encrypted with one or more additional keys.

Although the cited Sheer discusses encrypting a decrypting key block used to decrypt content on the disk with one or more keys, the Examiner has not cited any part of Shear that teaches that one key is associated with a plurality of storage cartridges, wherein this one key is used to code and decode data from the storage mediums of the storage cartridges.

Accordingly, Applicants submit that claim 3 provides additional grounds of patentability over the cited art because the cited Shear and O'Connor do not teach the additional requirements of these claims.

Claim 7 is amended to depend from claim 1 and to recite that encrypting the coding key comprising encrypting, by the host, the coding key. This added requirement is disclosed in at least paras. 50-51 and FIGs. 11 and 13 of the Specification.

Claim 8 is amended to depend from claim 1, to remove the "transmitting the coding key" limitation, and that the host uses a second key to decrypt the coding key encrypted with the first key, and that the host encrypts the coding key by encrypting the coding key with a third key, where the interface device uses a fourth key to decrypt the coding encrypted with the host third key. This added requirement is disclosed in at least paras. 50-51 and FIGs. 11 and 13 of the Specification.

The Examiner cited FIGs. 1A, 1B, 1C and paras. 0078-0081, 0127-0138, 0183, 0193-0199, and 0216-0220 of Shear as disclosing the requirements of the pre-amended claim 8. (Office Action, pgs. 7-8) Applicants traverse with respect to the amended claims.

The cited para. 0078 discusses rights management to exchange movies and games. Content is encrypted with decryption keys required to decrypt the content. The decryption keys may themselves be encrypted in an encrypted key block. The cited para. 0079 mentions that content may be secured as it is recording, such as in a camera. Reading the content for use in the rights management environment might occur at many steps along a conventional production and distribution process. Para. 0080 mentions that the storage medium carries the decryption key in a hidden portion that is used by a drive to decrypt the encrypted key block. The cited para. 0081 mentions that the video disk drive may store keys to decrypt an encrypted key block or the may be stored in a drive key store and be updateable.

The cited paras. 0127-0138 mention that different information on the medium may be encrypted using different keys and that encrypted keys may be stored on the medium to be used to decrypt the protected properties and metadata. Multiple sets of encrypted keys may be stored on the medium to have different keys associated with different regions. A decryption key for the encrypted keys may be hidden on the medium.

The cited para. 0183 mentions that a disk may store properties or other content in protected or unprotected form, where a property is protected if it is at least in part encrypted.

The disk could store both a movie as protected property and an unprotected interview, and store any number of protected or unprotected properties.

The cited paras. 0193-0199 discuss local secure execution of a control process and the use of optical media. Special hardware can be used to provide a secure execution environment to ensure safe digital commerce activities. A metering and control system, at least partially encrypted, is delivered to a user on optical media. A bill may be generated in response to transmitting information. Some or all of the content may be encrypted on the media.

The cited paras. 0216-0220 further discusses that the disk may store an encrypted key block used to decrypt properties and metadata on the disk, where different keys may be used for different data on the disk. The cited para. [0217] mentions that the cryptographic key block, which is the key used to decrypt the data, may be encrypted with one or more additional keys, and that these one or more keys need to be used to decrypt the key block to obtain the key to decrypt the data. The cited paras. [0218-0220] mentions that the keys to decrypt the encrypted key block may come from different sources. The disk may store hidden keys or the keys may be provided by the disk drive. The disk drive may have an integrated circuit decryption engine including a small secure internal key store memory having keys to use to decrypt the encrypted key block, which is then used to decrypt the content. The keys to decrypt the protected content may also be within a secure container.

The above cited Sheer discusses that a drive may access an encrypted key from disk and use the key do decrypt data from the disk. The cited para. [0081] further mentions that the disk drive may store and maintain keys used to decrypt an encrypted key block, and that a drive key store may be updateable using a communication path. The cited para. [0217] mentions that the key block having the key to decrypt the data may be encrypted with one or more additional keys.

Although the cited Sheer discusses encrypting a decrypting key block used to decrypt content on the disk with one or more keys, the Examiner has not cited any part of Shear that teaches encrypting the coding key with a first key, where the host uses a second key to decrypt the coding key, and that the host encrypts the coding key with a third key, and that the interface device, or cited drive, uses a fourth key the key that is then used to decrypt the coding key, or cited encrypted key block.

Accordingly, Applicants submit that claim 8 provides additional grounds of patentability over the cited art because the cited Shear and Smythe do not teach the additional requirements of these claims.

Amended independent claim 10 recites a method performed by an interface device for accessing data in a removable storage cartridge including a read/write storage medium coupled to the interface device, comprising: receiving an encrypted coding key from a host system with an Input/Output (I/O) request directed to the storage cartridge; mounting the storage cartridge in response to the I/O request; decrypting the encrypted coding key; using the decrypted coding key to encode data to write to the storage medium in response to the I/O request comprising a write request; using the decrypted coding key to decode data written to the storage medium in response to the I/O request comprising a read request; and storing the received encrypted coding key in the storage medium to use for subsequent I/O requests.

Applicants amended claim 10 to add the requirement that an encrypted coding key is received from a host system with an Input/Output (I/O) request directed to the storage cartridge; mounting the storage cartridge in response to the I/O request. These added requirements are disclosed in at least paras. 14-18 and paras. 55-66 of the Specification.

The Examiner cited the above discussed FIGs. 1A, 1B, 1C and paras. 0078-0081, 0127-0138, 0183, 0193-0199, and 0216-0220 of Shear as disclosing the requirements of the pre-amended claims. (Office Action, pg. 8)

Applicants submit that the Examiner has not cited any part of Shear that teaches or suggests an interface device for accessing a coupled storage medium receive an encrypted coding key from a host with an I/O request directed to the storage cartridge, mounting the storage cartridge in response to the received I/O request, decrypting the encrypted coding key, and using the coding key to encode data to write to the storage medium for a write I/O request and decode data read from the storage for a read I/O request. Instead, as discussed, the cited Shear discusses a drive accessing an encrypted decrypting key to use to decrypt content on a disk (DVD). This does not disclose decrypting the encrypted encoding key received from a host system with an I/O request directed to the storage cartridge to use encode data to write to the storage medium in the storage cartridge for an I/O request.

Further, the Examiner has not cited any part of Shear that teaches the claim requirement of storing the received encrypted coding key in the storage medium to use for subsequent I/O requests. The above cited Sheer discusses that a drive may access an encrypted key from disk and use the key do decrypt data from the disk. The cited para. [0081] further mentions that the disk drive may store and maintain keys used to decrypt an encrypted key block, and that a drive key store may be updateable using a communication path. The cited para. [0217] mentions that

the key block having the key to decrypt the data may be encrypted with one or more additional keys. However, these cited sections do not disclose that the disk drive, which decrypted and used a key to code data to write to the storage, stores an encrypted coding key received from a host system with an I/O request in the storage medium for subsequent I/O requests.

Accordingly, for the above reasons, Applicants submit that the independent claim 10 is patentable over the cited art because the cited Shear and Smythe do not teach or suggest all the claim requirements.

Claims 11-16 are patentable over the cited art because they depend from claims 10, which is patentable over the cited art for the reasons discussed above. Moreover, the below discussed dependent claims provide additional details grounds of patentability over the cited art.

Claim 12 was amended to recite maintaining, by the interface device, a second key to decrypt data encrypted using the first key, wherein the interface device uses the second key ~~is used~~ to decrypt the coding key encrypted with the first key. These added requirements are disclosed in at least paras. 14-18 and paras. 55-66 of the Specification.

Amended claim 16 depends from claim 10 and further require that the received encrypted coding key is encrypted by a first key maintained at the host system, wherein the host system maintains a second key to decrypt data encrypted using the first key, wherein the interface device decrypts the encrypted coding key by: receiving, with the I/O request, from the host system, the second key encrypted by the host system using a third key, wherein data encrypted using the third key is decrypted using a fourth key; accessing the fourth key; using the fourth key to decrypt the encrypted second key received from the host system; and using the decrypted second key to decrypt the received coding key encrypted using the first key.

The added requirements that the interface device decrypts the encrypted coding key by performing the operations and that the second key is received with the I/O request. These added requirements are disclosed in at least paras. 14-18 and paras. 55-66 of the Specification.

The Examiner cited the above discussed sections of Shear with respect to these claims. (Office Action, pg. 10)

Applicants submit that the Examiner has not cited any part of Shear that teaches that the coding key, corresponding to the cited decryption key, is encrypted with a first key and that the interface device receives a second key encrypted with a third key that it decrypts with a fourth key to then use the second key to decrypt encrypted coding key to use. For instance, the Examiner has not cited where Shear discloses that the disk drive receives a further key that is

used to decrypt the key it maintains to use to decrypt the key block on the DVD. Instead, the cited Shear, including para. 0217 mentions that the key block having the key to decrypt the data may be encrypted with one or more additional keys.

Accordingly, Applicants submit that claim 16 provides additional grounds of patentability over the cited art because the cited Shear does not disclose the additional requirements of these claims.

3. Added Claim 45-74

Added claim 45 depends from claim 1 and further requires that the first key comprises a host public key, wherein the second key comprises a host private key, wherein the third key comprises an interface device public key and wherein the fourth key comprises an interface device private key.

Added claim 46 depends from claim 16 and further requires wherein the first key comprises a host public key, wherein the second key comprises a host private key, wherein the third key comprises an interface device public key and wherein the fourth key comprises an interface device private key.

The requirements of added claims 45 and 46 are disclosed in at least paras. 50-51 and FIGs. 11 and 13.

Claims 47-59 include the requirements of claims 1, 3, 4, 7, 8, 44, 10, 12-16, and 46 in system form. Claims 60-75 include the requirements of claims 1, 3-5, 7, 8, 44, 45, 10-16, and 46 in article of manufacture form. The preamble and additional requirements of the system and article of manufacture claims are disclosed in at least FIGs. 10, 11, 14, 16, 18, and paras. 43, 44, 47, 55, 59, 63, and 69 of the Specification.

Added claim 45 is patentable over the cited art because it depends from claim 1 and the additional requirements of claim 45 in combination with the base claims provide further grounds of patentability over the cited art.

Added claims 47-75 are patentable over the cited art because they include requirements of claims 1, 3, 4, 7, 8, 44, 45, 10-16, and 46, which are patentable over the cited art for the reasons discussed above.

Conclusion

For all the above reasons, Applicant submits that the pending claims 1, 3-5, 7, 8, 10-16, and 44 are patentable over the art of record. Should any additional fees be required, please charge Deposit Account No. 09-0466.

The attorney of record invites the Examiner to contact him at (310) 553-7977 if the Examiner believes such contact would advance the prosecution of the case.

Dated: March 18, 2009

By: /David Victor/

David W. Victor
Registration No. 39,867
Tel: 310-553-7977
Email: david@ipmatters.com